CLAIMS

What is claimed is:

1. A multi-word arithmetic device for executing modular arithmetic on multi-word integers, in accordance with instructions from an external device, the multi-word arithmetic device comprising:

a memory;

an arithmetic unit for executing, on word units, at least two types of calculation, including addition and multiplication, and outputting a one-word calculation result;

a memory input/output circuit for performing (1) a first data transfer for storing in the memory at least one integer received from an external device, (2) a second data transfer for inputting at least one integer stored in the memory into the arithmetic unit in word units, (3) a third data transfer for storing in the memory the calculation result output from the arithmetic unit, and (4) a fourth data transfer for outputting the calculation result from the memory to the external device; and

a control circuit for, according to instructions received from the external device,

(a) specifying, to the memory input/output unit, data to

be transferred by the second and third data transfers, and

(b) specifying, to the arithmetic unit, a type of calculation to be executed,

thereby controlling:

(i) the arithmetic unit to selectively perform one of at least two types of modular arithmetic on the at least one integer stored in the memory; and

(ii) the memory input/output circuit to store the calculation result of the modular arithmetic into the memory.

2. The multi-word arithmetic device of Claim 1, wherein

at least two integers are stored in the memory,

the arithmetic unit includes:

an adder for adding at least two pieces of one-word data; and

a multiplier for multiplying at least two pieces of one-word data, and

the memory input/output circuit simultaneously reads one word from each of the at least two integers stored in the memory, and outputs the read words to one of the adder and the multiplier.

3. The multi-word arithmetic device of Claim 2, wherein:

the memory is divided into two dual-port memories, each allowing access to two storage areas designated by two addresses, and allowing (1) two read operations, or (2) one read operation and one write operation to be performed simultaneously on word units; and

the at least two integers are stored in each dual-port memory so that the memory input/output circuit can simultaneously (1) read a piece of one-word data simultaneously from each of the integers stored in the two dual-port memories, and have the read pieces of data input into one of the adder and the multiplier, and (2) write a piece of one-word data output from one of the adder and the multiplier into one of the two dual-port memories.

4. The multi-word arithmetic device of Claim 1, wherein the arithmetic unit, according to instructions from the control circuit, executes one of the following three calculations: (1) addition of at least two pieces of one-word data; (2) multiplication of two pieces of one-word data; and (3) multiplication of two pieces of one-word data and accumulation of multiplication results.

5. The multi-word arithmetic device of Claim 4, wherein

the arithmetic unit includes:

a multiplier receiving an input of two pieces of one-word data and outputting a piece of two-word data;

an adder receiving an input of at least two pieces of two-word data, including a piece of two-word data output from the multiplier, and outputting a piece of multi-word data; and

a selecting circuit selecting, according to instructions from the control circuit:

(1), data to be input into one of the multiplier and the adder out of data transmitted from the memory input/output circuit; and

(2) data to be output as the calculation result out of data output from one of the adder and the multiplier.

6. The multi-word arithmetic device of Claim 1, wherein the at least two types of modular arithmetic include modular addition, and

on receiving, from the external device, an instruction to execute modular addition and an indication of a number of words *n* for each integer on which modular addition is to be performed, the control circuit controls the memory input/output circuit and the arithmetic unit to execute the following processing:

(1) the memory input/output circuit obtains from the external device and stores in the memory two *n*-word integers A and B on which modular addition is to be executed and a *n*-word integer P showing a modulus;

(2) the memory input/output circuit (a) reads simultaneously, from the integers A, B and P stored in the memory, pieces of one-word data *a*, *b* and *p*, each with a same digit position, and has the read pieces of data input into the arithmetic unit, while (b) storing in the memory a piece of one-word data *w* output from the arithmetic unit, and repeats processes (a) and (b) sequentially from a lowest-order word in each integer until *n* words of data are obtained, enabling an *n*-word integer W to be stored in the memory; and

(3) the arithmetic unit repeats *n* times a process in which the pieces of data *a*, *b* and *p* received from the memory input/output circuit are computed as $a + b - p$, propagating a carry, and a result *w* is output.

7. The multi-word arithmetic device of Claim 6, wherein the control circuit determines whether a carry has been generated by the arithmetic unit immediately after completion of the processing (1) to (3) and if a carry has been generated, further controls the memory input/output circuit

and the adder to execute the following processing:

(4) the memory input/output circuit (a) reads simultaneously, from the integers W and P stored in the memory, pieces of one-word data *w* and *p*, each with a same digit position, and has the read pieces of data input into the arithmetic unit, while (b) storing in the memory a piece of one-word data *c* output from the arithmetic unit and repeats processes (a) and (b) sequentially from a lowest-order word in each integer until *n* words of data are obtained, enabling an *n*-word integer C to be stored in the memory; and

(5) the arithmetic unit repeats *n* times a process in which the pieces of data *w* and *p* received from the memory input/output circuit are computed as *w* + *p*, propagating a carry, and a result *c* is output.

8. The multi-word arithmetic unit of Claim 1, wherein the at least two types of modular arithmetic include Montgomery reduction calculating a residue for A·R^(-1) mod P, when each word has *k* bits, A is a 2*n*-word integer used for input data, R is an integer 2^(*k*×*n*) and P is an *n*-word integer; and

upon receiving, from the external device, an instruction to execute Montgomery reduction and an indication of a number of words 2*n* for an integer A on which Montgomery reduction is to

be performed, the control circuit controls the memory input/output circuit and the arithmetic unit to execute Montgomery reduction.

9. The multi-word arithmetic device of Claim 8, wherein, when receiving an instruction to execute Montgomery reduction from the external device, the control circuit controls the memory input/output circuit and the arithmetic unit so as to execute the following processing:

(1) the memory input/output circuit acquires integers A, P and V from the external device and stores the obtained integers in the memory, the integer V being -P^(-1) mod R;

(2) the arithmetic unit computes partial products for words from each of (i) a lower *n* words of the integer A stored in the memory, and (ii) the integer V, and accumulates words in partial products having a same digit position, repeating the process sequentially from a lowest word in each integer until *n* words of accumulated results are obtained, and storing the accumulated results in the memory as a piece of *n*-word intermediate data B;

(3) the arithmetic unit computes partial products for words from each of (a) the piece of intermediate data B and (b) the integer P stored in the memory, and accumulates words in the

partial products having a same digit position so that, when a lowest word is a 0th word, accumulated results for a 0th to (n-3)th word are not obtained, but accumulated results for a (n-2)th word to a (2n-1)th word are obtained and stored in the memory as the upper (n+1) words of a piece of intermediate data D;

(4) the arithmetic unit (a) generates (i) a carry obtained from a one-word addition performed by adding a lowest word from each of the piece of intermediate data D and an integer AA, and (ii) a one-bit logical value, the integer AA being an upper (n+1) words of the integer A, and the one-bit logical value being 0 when a one-word addition result is 0, and 1 when the one-word addition result is not 0, and (b) adds an upper n words of the piece of intermediate data D, an upper n words of the integer AA, the carry and the one-bit logical value, by repeating addition of word units sequentially from a lowest word in each integer, while propagating a carry, until n words of data are obtained, and stores an addition result in the memory as a piece of n-word output data M; and

(5) when the output data M stored in the memory is at least as large as the integer P, the arithmetic unit subtracts the integer P from the output data M until the output data M is 0 or a positive integer smaller than the integer P, by repeating

subtraction of word units sequentially from a lowest word in each integer, while propagating a carry, until *n* words of data are obtained, and stores the subtraction results in the memory as a new piece of *n*-word output data M.

10. The multi-word arithmetic device of Claim 9, wherein in processing (4), the arithmetic unit adds a piece of one-word data containing all ones to the piece of intermediate data D and the integer AA, and stores an upper *n* words of an obtained addition result in the memory as the output data M.

11. The multi-word arithmetic device of Claim 10, wherein, in processing (2) and (3), the arithmetic unit selects sets of word pairs, each set formed from all the pairs of words that generate a partial product with a same digit position, sets input values in the multiplier, and computes and accumulates the partial products for the selected pairs of words in sequence from the set with a lowest digit position.

12. The multi-word arithmetic device of Claim 11, wherein, in processing (2) and (3), the arithmetic unit stores in the memory as part of a multiplication result a lower word from a two-word accumulated result obtained by accumulating partial

products with the same digit position, and adds an upper word from the accumulated result to partial products that have a digit position one word higher and are thus the next to be calculated.

13. The multi-word arithmetic device of Claim 12, wherein the arithmetic unit performs an operation for storing a lower word from the accumulated result in the memory simultaneously with an operation for adding an upper word from the accumulated result to partial products that have a digit position one word higher and are thus the next to be calculated.

14. The multi-word arithmetic device of Claim 10, wherein, when computing and accumulating partial products in processing (2) and (3), the arithmetic unit updates accumulated values by (a) simultaneously (i) computing a partial product and (ii) reading a previously accumulated one-word value from the memory, (b) adding the accumulated one-word value to a corresponding word in the partial product, and (c) storing a result of the addition in a corresponding area of the memory.

15. A multi-word arithmetic device for executing modular

arithmetic on multi-word integers, in accordance with instructions from an external device, the multi-word arithmetic device comprising:

a memory;

an arithmetic unit for executing, on word units, at least two types of calculation, including addition and multiplication, and outputting a one-word calculation result;

a memory input/output circuit for performing (1) a first data transfer for storing in the memory at least one integer received from an external device, (2) a second data transfer for inputting at least one integer stored in the memory into the arithmetic unit in word units, (3) a third data transfer for storing in the memory the calculation result output from the arithmetic unit, and (4) a fourth data transfer for outputting the calculation result from the memory to the external device; and

a control circuit for, according to instructions received from the external device,

(a) specifying, to the memory input/output unit, data to be transferred by the second and third data transfers, and

(b) specifying, to the arithmetic unit, a type of calculation to be executed,

thereby controlling:

(i) the arithmetic unit to selectively perform one of at least two types of modular arithmetic on the at least one integer stored in the memory; and

(ii) the memory input/output circuit to store the calculation result of the modular arithmetic into the memory,

wherein the at least two types of modular arithmetic include modular addition and Montgomery reduction; and

the control circuit controls the memory input/output circuit and the arithmetic unit so that the arithmetic unit (1) computes A+B mod P when an instruction for executing modular addition is received from the external device, A, B and P being *n*-word integers, and (2) computes a residue for A·R^(-1) mod P, when an instruction for executing Montgomery reduction is received from the external device, each word having *k* bits, A being a 2*n*-word integer used as input data, R being an integer 2^(*k*×*n*) and P being an *n*-word integer.

16. The multi-word arithmetic unit of Claim 15, wherein the arithmetic unit includes:

a multiplier receiving an input of two pieces of one-word data and outputting a piece of two-word data;

an adder receiving an input of at least two pieces of two-word data, including a piece of two-word data output from the

multiplier, and outputting a piece of multi-word data; and

a selecting circuit selecting, according to instructions from the control circuit:

(1), data to be input into one of the multiplier and the adder out of data transmitted from the memory input/output circuit; and

(2) data to be output as the calculation result out of data output from one of the adder and the multiplier.

17. The multi-word arithmetic unit of Claim 16, wherein the memory is divided into two dual-port memories, each allowing access to two storage areas designated by two addresses, and allowing (1) two read operations, or (2) one read operation and one write operation to be performed simultaneously on word units; and

the at least two integers are stored in each dual-port memory so that the memory input/output circuit can simultaneously (1) read a piece of one-word data simultaneously from each of the integers stored in the two dual-port memories, and have the read pieces of data input into one of the adder and the multiplier, and (2) write a piece of one-word data output from one of the adder and the multiplier into one of the two dual-port memories.